CLAIMS

1. An outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsource source encryption device comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to generate second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

2. The outsource source encryption device of Claim 1, wherein

the generating unit uses individual information particular to the outsource source encryption device to generate certification information based on the first license information, and

the second license information further includes the certification information.

3. The outsource source encryption device of Claim 2, wherein

the generating unit generates the certification information based on identification information of the outsource destination

encryption device and the first license information.

4. The outsource source encryption device of Claim 2, wherein the certification information is a certifier generated using secret key encryption, and

the individual information is a secret key used in the secret key encryption.

5. The outsource source encryption device of Claim 2, wherein the certification information is digital signature data generated using public key encryption, and

the individual information is a secret key used in the public key encryption.

6. The outsource source encryption device of Claim 1, wherein the first license information includes certification information generated using individual information particular to the content distribution device.

7. The outsource source encryption device of Claim 6, wherein the certification information is generated based on identity information of the outsource source encryption device.

8. The outsource source encryption device of Claim 7, wherein the certification information is a certifier generated using secret key encryption, and

the individual information is a secret key used in the secret key encryption .

9. The outsource source encryption device of Claim 7, wherein the certification information is digital signature data generated using public key encryption, and

the individual information is a secret key of the public key encryption.

10. The outsource source encryption device of Claim 1, wherein the receiving unit further receives fourth license information that includes third license information proving that another encryption device has permission to use the content from a content distribution device and proves that the other encryption device has outsourced the encryption of the content to the outsource source encryption device,

the generating unit generates fifth license information that includes the fourth license information and proves that encryption has been outsourced to the outsource destination encryption device, and

the transmission unit transmits the fifth license information together with the content to the outsource destination encryption device.

11. A key distribution device that distributes key data used in encryption of content to encryption devices, the key distribution device comprising:

an acquiring unit operable to acquire second license information that includes first license information proving that the first encryption device is permitted to use the content and proves

that encryption of the content has been outsourced from a first encryption device to a second encryption device;

a judging unit operable to judge whether or not the second license information was generated by the first encryption device; and

a transmission unit operable to transmit the key data to the second encryption device if a result of the judgment is in the affirmative.

12. The key distribution device of Claim 11, wherein

the second license information includes certification information generated for the first license information using individual information particular to the first encryption device, and

the judging unit holds verification information corresponding to the individual information, and judges using the verification information.

13. The key distribution device of claim 12, wherein

the certification information is generated from the first license information and the identity information of the second encryption device.

14. The key distribution device of claim 12, wherein

the certification information is a certifier generated using secret key encryption,

the individual information is a secret key used in the secret key encryption,

the judging unit generates the certifier by performing an algorithm in substantially the same way as the secret key encryption is performed on the first license information, and judges whether or not the generated certifier and a received certifier match, and

when the generated and received certifiers match, judges that the second license information was generated by the first encryption device.

15. The key distribution device of Claim 12, wherein

the certification information is digital signature data generated using public key encryption,

the individual information is a secret key used in the public key encryption,

the verification information is a public key corresponding to the secret key, and

the judging unit performs verification on the digital signature data using the public key, and if a verification result indicates successful verification, judges that the second piece of license information was generated by the first encryption device.

16. The key distribution device of Claim 11, wherein

the acquiring unit further acquires third license information that includes the second license information and proves that the encryption of the content has been outsourced from the second encryption device to a third encryption device,

the judging unit further judges whether or not the third license information was generated by the second encryption device, and

the transmission unit further transmits the key data to the

third encryption device if the judgment result is in the affirmative.

17. The key distribution device of Claim 11, further comprising an acquired information judging unit that judges which of the first license information and the second license information the acquiring unit has received, wherein

the judging unit,

when the judgment result from the acquired information judging unit indicates that the first piece of license information has been received, judges whether or not the first license information was generated by the content distribution device which distributes the content, and

when the judgment result indicates that the second piece of license information has been received, judges whether or not the second license information was generated by the first encryption device, and

the transmission unit,

when the judgment result from the acquired information judging unit indicates that the first license information has been received, transmits the key data to the first encryption device, and

when the judgment result indicates that the second license information was received, transmits the key data to the second encryption device.

18. The key distribution device of Claim 17, wherein

the acquired information judging unit judges that the first license information was received if the data size of the acquired information is less than or equal to a predetermined value, and judges

that the second license information was received if the data size is greater than the predetermined value.

19. The key distribution device of Claim 11, further comprising:

a key holding unit operable to hold an individual key also held by the second encryption device, the individual key being particular to the second encryption device; and

an encryption unit operable to encrypt the key data using the individual key to generate encrypted key data, wherein

the transmission unit transmits the encrypted key data to the second encryption device as the key data.

20. A key distribution system that distributes key data for using content, the key distribution system comprising:

an outsource source encryption device operable to receive first license information proving that the outsource source encryption device is permitted to use the content, generate second license information that includes the first license information and proves that encryption of the content has been outsourced to an outsource destination device, and transmit the generated second license information together with received content to the outsource destination encryption device;

an outsource destination encryption device operable to receive the second license information together with the content, transmit the received second license information to a key distribution device and receive the key data from the key distribution device; and

a key distribution device operable to receive the second license

information, judge whether or not the second license information was generated by the first encryption device, and transmit the key data to the second encryption device when the judgment is in the affirmative.

21. An integrated circuit used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the integrated circuit comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to generate second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

22. An integrated circuit used in a key distribution device that distributes key data used in encryption of content to encryption devices, the integrated circuit comprising:

an acquiring unit operable to acquire second license information that proving that encryption of the content has been outsourced from a first encryption device to a second encryption device, the second license information including first license

information proving that a first encryption device is permitted to use the content;

a judging unit operable to judge whether or not the second license information has been generated from the first license information; and

a transmission unit operable to transmit the key data to the second encryption device if the result of the judgment is in the affirmative.

23. An outsourcing method used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsourcing method comprising steps of:

a receiving unit receiving first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit generating second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and

a transmission unit transmitting the generated second license information together with the received content to the outsource destination device.

24. An outsourcing program used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of

the received content to an outsource destination encryption device, the outsourcing program comprising:

a receiving step of a receiving unit receiving first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating step of a generating unit generating second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and

a transmission step of a transmission unit transmitting the generated second license information together with the received content to the outsource destination device.

25. A computer readable recording medium on which is recorded an outsourcing program used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsourcing program comprising:

a receiving step of a receiving unit receiving first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating step of a generating unit generating second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and

a transmission step of a transmission unit transmitting the generated second license information together with the received

content to the outsource destination device.

26. A key distribution method used in a key distribution device that distributes key data used in encryption of content to encryption devices, the key distribution method comprising steps of:

an acquiring unit acquiring second license information that includes first license information proving that the first encryption device is permitted to use the content and proves that encryption of the content has been outsourced from a first encryption device to a second encryption device;

a judging unit judging whether or not the second license information was generated by the first encryption device; and

a transmission unit transmitting the key data to the second encryption device if a result of the judgment is in the affirmative.

27. A key distribution program used in a key distribution device that distributes key data used in encryption of content to encryption devices, the key distribution program comprising:

an acquiring step of an acquiring unit acquiring second license information that includes first license information proving that the first encryption device is permitted to use the content and proves that encryption of the content has been outsourced from a first encryption device to a second encryption device;

a judging step of a judging unit judging whether or not the second license information was generated by the first encryption device; and

a transmission step of a transmission unit transmitting the key data to the second encryption device if a result of the judgment

is in the affirmative.

28. A computer readable recording medium on which is recorded a key distribution program used in a key distribution device that distributes key data used in encryption of content to encryption devices, the key distribution program comprising:

an acquiring step of an acquiring unit acquiring second license information that includes first license information proving that the first encryption device is permitted to use the content and proves that encryption of the content has been outsourced from a first encryption device to a second encryption device;

a judging step of a judging unit judging whether or not the second license information was generated by the first encryption device; and

a transmission step of a transmission unit transmitting the key data to the second encryption device if a result of the judgment is in the affirmative.

29. License data indicating that encryption of content is to be outsourced from an encryption device with permission from a content distribution device to encrypt the content to another encryption device, the license data comprising:

first license information proving that an source encryption device has permission from a content distribution device to use the content; and

second license information that is generated based on the first license information, and proves that the outsource source encryption device has outsourced encryption of the content to a destination

encryption device.

30. The license data of Claim 29, wherein

the first license information is at least one of a digital signature and a certifier, and is generated by the content distribution device; and

the second license information is at least one of a digital signature and a certifier generated for the first license information by the outsource source encryption device that received the first license from the content distribution device.

31. The license data of Claim 29, wherein

the license data is recorded on a recording medium.